Defense in Depth:

Securing the Desktop in a Managed Environment

3com

Jeff Stevenson
Federal Network Consultant
jeff_stevenson@3com.com
NMCI Symposium
June 18, 2003

Network Security is a Serious Issue

- $202 Billion Lost Every Year by Companies to “Cybercrime”
- *90% of cybercrime financial losses are INTERNAL (intranets)*
- U.S. Government alone will experience over 300,000 Internet attacks this year
- Over 400,000 WWW pages contain some form of Hacker Tools
- Cybercrimes are estimated to take place every 20 seconds...

Network attacks by insiders are a real thre

- Computer Crime and Security Survey 2001
  - Joint CSI/FBI survey of 538 US organizations
    - 97% with Web sites
    - 47% provide electronic commerce services
- 78% reported financial losses due to attacks
  - Only 37% could quantify loss monetarily
  - $377 million in total losses reported
- ***49% reported incidents of unauthorized network access by insiders***

Source: Computer Crime and Security Survey 2001

Know Who's on Your Network– Robert Hanssen

Unauthorized access to:

- The National Measurement and Signature Intelligence Program, involving acoustic intelligence, radar intelligence and nuclear radiation detection.
- The FBI Double Agent Program.
- The Intelligence Community's Comprehensive Compendium of Future Intelligence Requirements.
- A study on recruitment operations of the KGB against the CIA.
- An assessment of the KGB's effort to gather information on U.S. nuclear programs.
- A CIA analysis of the KGB's First Chief Directorate (FCD), its international intelligence division.
- FBI counterintelligence techniques, sources, methods and operations. .

"In one case, he compromised an entire technical program of enormous value, expense and importance to the United States Government," the affidavit states.

Networked Servers

What are we protecting?

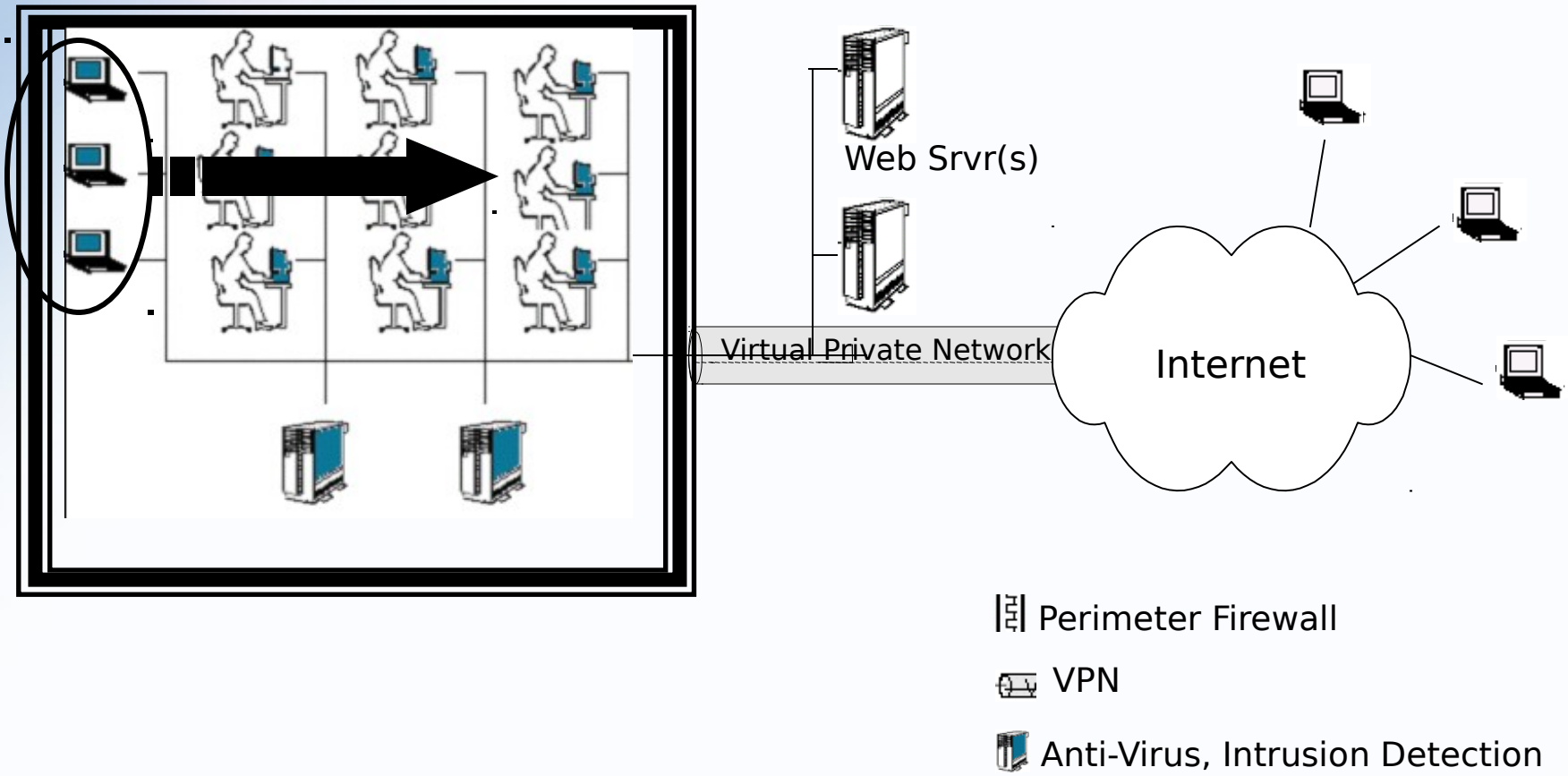
- Information Servers
- Infrastructure Servers
- Applications Servers

Security is required to protect the privacy and integrity of server contents and to ensure that network resources & business process availability are not compromised

Typical Attacks

- Insider attack
- Social engineering
- Virus infiltration
- Denial of Service
- OS or application bug
- Infiltration via passwords
- Infiltration via “no security”
- Spoofing
- Trojan horse
- Brute force
- Stealth infiltration
- Protocol flaw or exploit

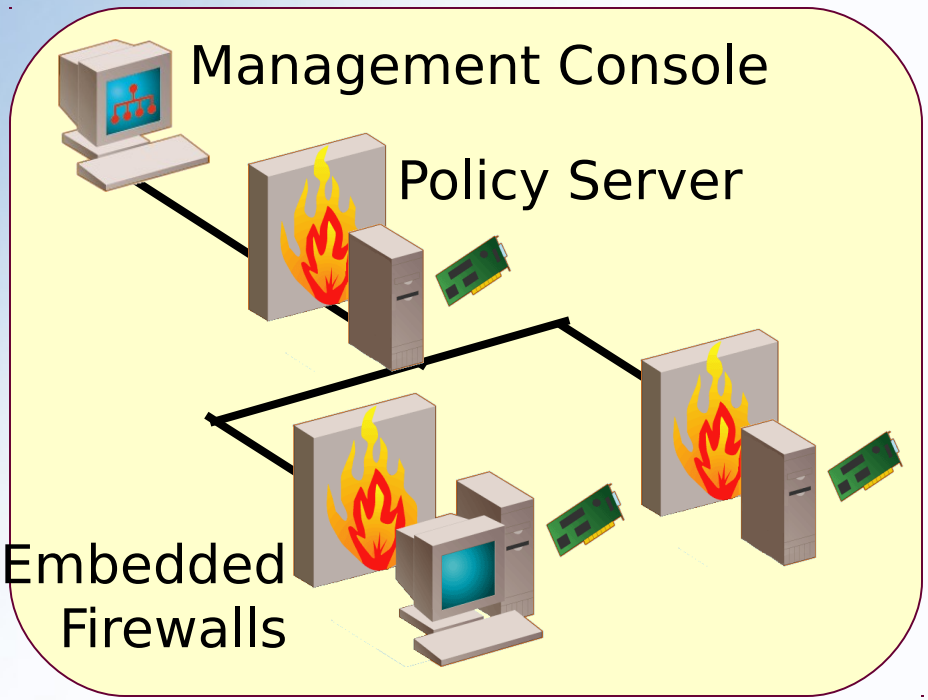
Current Network Security The 'Big Picture'



Current Network Picture

- Perimeter Firewalls
- Departmental Firewalls
  - Assume all hacking is inter-departmental
  - Topology Dependent
  - Don’t provide for sniffing/spoofing protection
  - Don’t harden individual hosts
- Intrusion Detection Systems
  - Only “detects” and do not “protect”
  - IDS “signatures” have to be updated
  - Only deal with known protocol deficiencies or known applications
  - IDS can be “Noisy”, forwarding many “False Positives”
- Distributed anti-virus
  - Signature based and needs to be updated

Introducing the 3Com Embedded Firewall



- Implements distributed tamper-resistant firewalls at the NIC
- Enforces security policy at the network connection
- Limits network access on a “need-to-know” basis
- Creates protected enclaves
- Provides intrusion resistance
- Allows for asset management

Introducing Hardware Based Distributed Firewalls

- 3Com Firewall Cards with 10/100 LAN
  - Embedded Firewall
  - With security co-processor
  - Offload IPSec to the card (VPN Acceleration)
- Centrally managed policies on remote machines
- Easy deployment, manageability and upgradeable
  - Via policy server which manages servers, desktop and laptops
- Tamper Resistance
  - Cannot be turned off by malicious code
  - Policy cannot be changed or disabled by user
  - HW based Firewall

DARPA Is Excited About Embedded Firewall

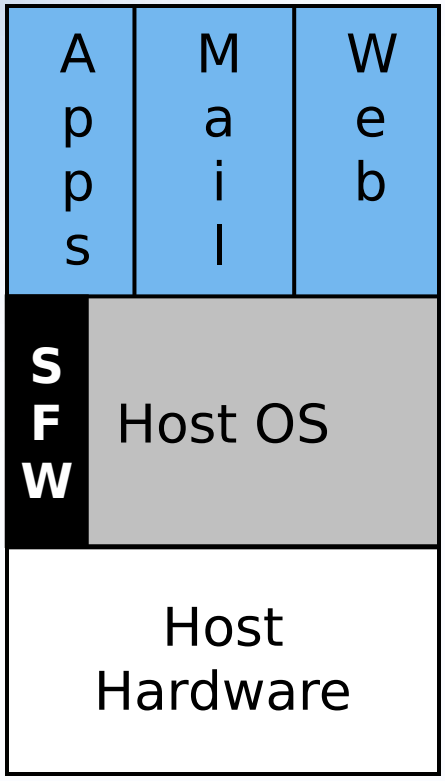
- "EFW demonstration tremendously successful… identified by the U.S. Navy as the most promising technology. The Navy has begun the process of programming and budgeting to buy these EFW's *in bulk*."
  - April 2002 DARPA Fact File
  - http://www.darpa.mil/body/Newsitems/darpa_fact.html

- "Distributed firewall technology places a firewall inside every computer on a network…providing much more robust protection than a single network firewall."
  - April 2002 Testimony to U.S. Con

EFW Combines the Best of Hardware and Software

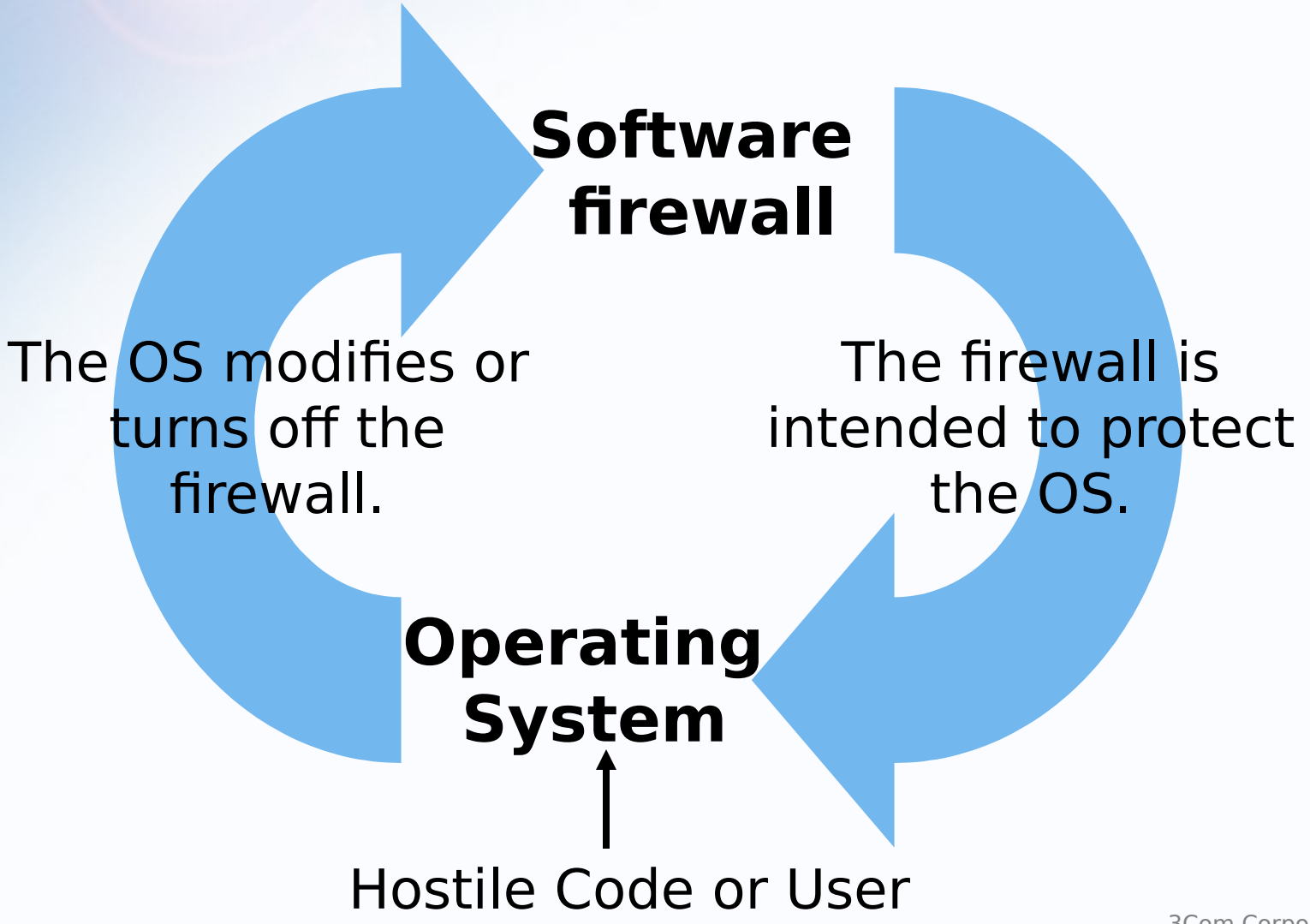
- EFW provides the advantages of hardware security
  - Unlike software firewalls, EFW is extremely tamper resistant
    - “Throwing more security software at a security problem that is caused by the essentially insecure nature of software is like going to a blind barber -- it can only end badly and, more likely than not, bloodily.” - Software Security is Soft Security - John Pescatore, Gartner Research Vice President
- EFW also allows the flexibility, mobility and central management of distributed software

Implementation approaches: software/personal firewall

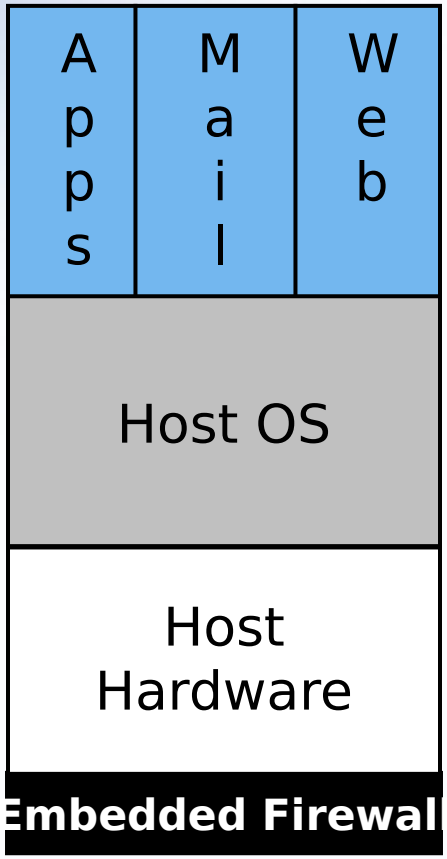


- Protects the local OS and applications from network attacks
- Firewall actions visible to OS, applications, and users
- Relies on OS for firewall integrity
- Attacker or applications could bypass or interfere
- User may have some control over rules within software
- Successful external attacks demonstrated

Vulnerabilities of software firewalls



Implementation approaches: Embedded Firewall



- Firewall actions transparent to OS, applications, and users
- Independent of local OS
- Unable to Bypass
- Tamper-resistant
- User has no control over rules
  - Centrally managed
- Secure against external attack
- Examples: 3Com Embedded Firewall

Superiority of Embedded Firewalls

Operating System

OS sends information to embedded hardware for examination

Packets intercepted and examined before being sent to OS

Embedded Firewall

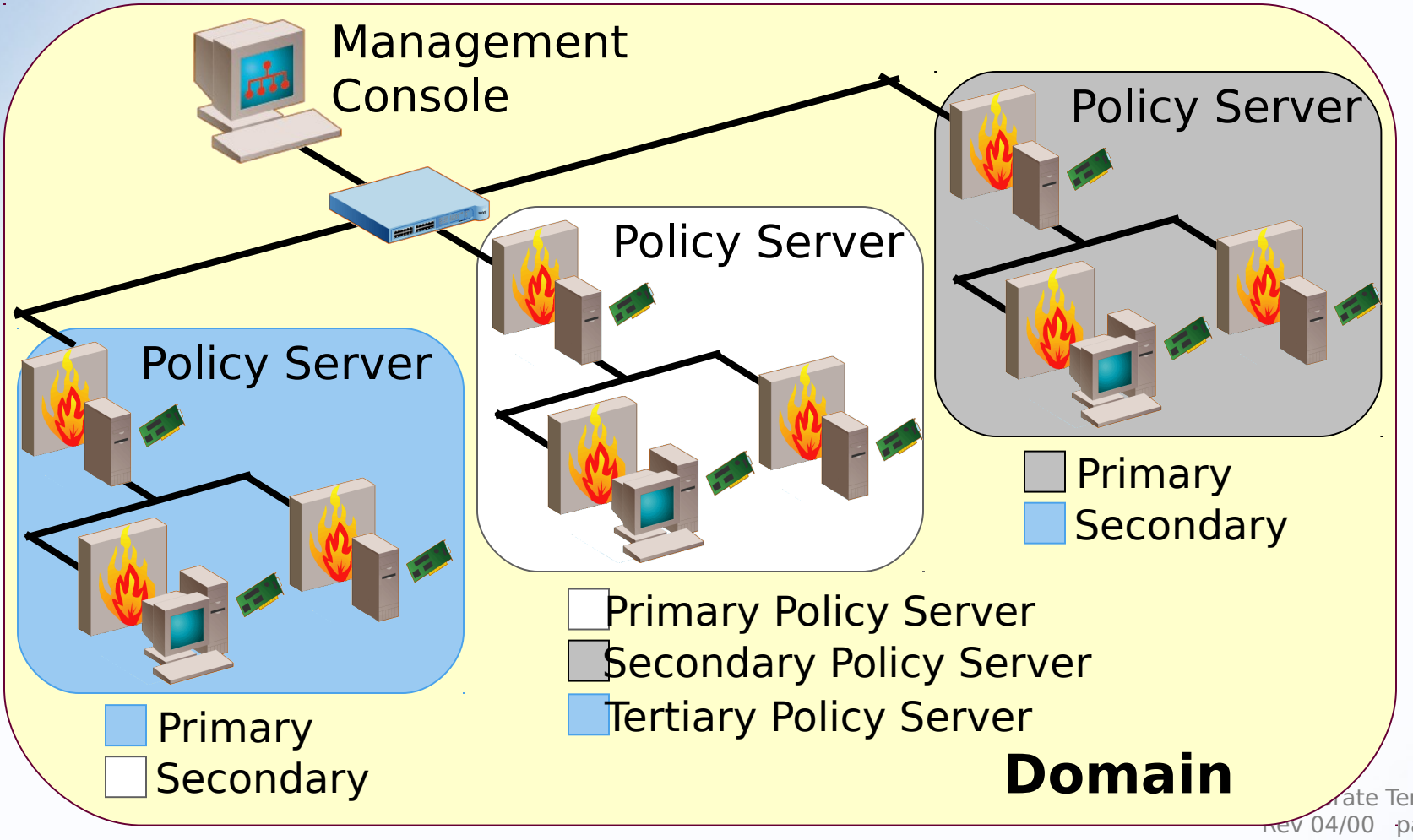
Hostile Code or User

Components of the 3Com Embedded Firewall

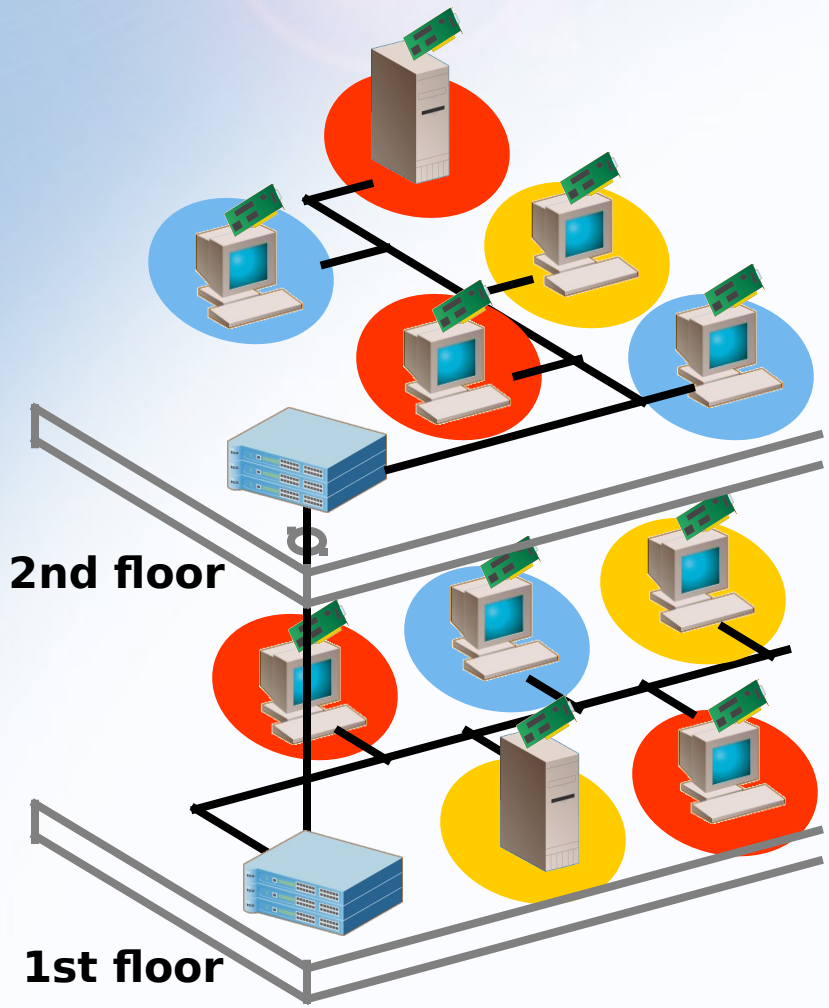
- Policy Server
  - Centrally creates, defines and distributes security policies to the NICs
- Management Console
  - Provides intuitive user interface
- 3Com 10/100 Secure NICs with Embedded Firewall
  - Executes the packet filtering rules dictated to it by the Policy Server

Embedded Firewall Domain

Up to 3 Policy Servers per domain



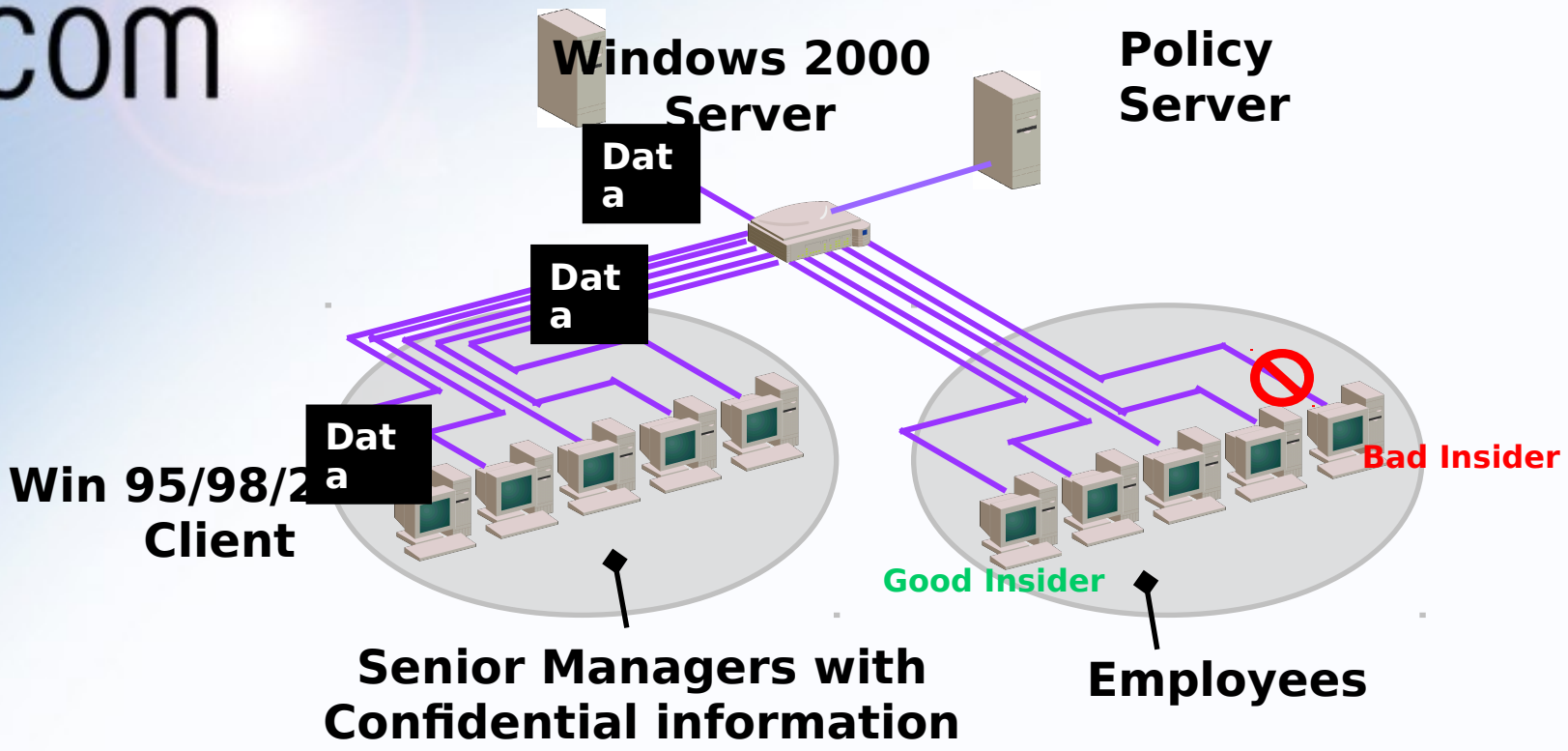
Create Protected Enclaves



- Provides access on a “need-to-know” basis…
- Topology independent
  - Don’t need to configure at every point in the path
  - Policies are role based
- Enclaves can limit access to:
  - Individual devices
  - Host based applications

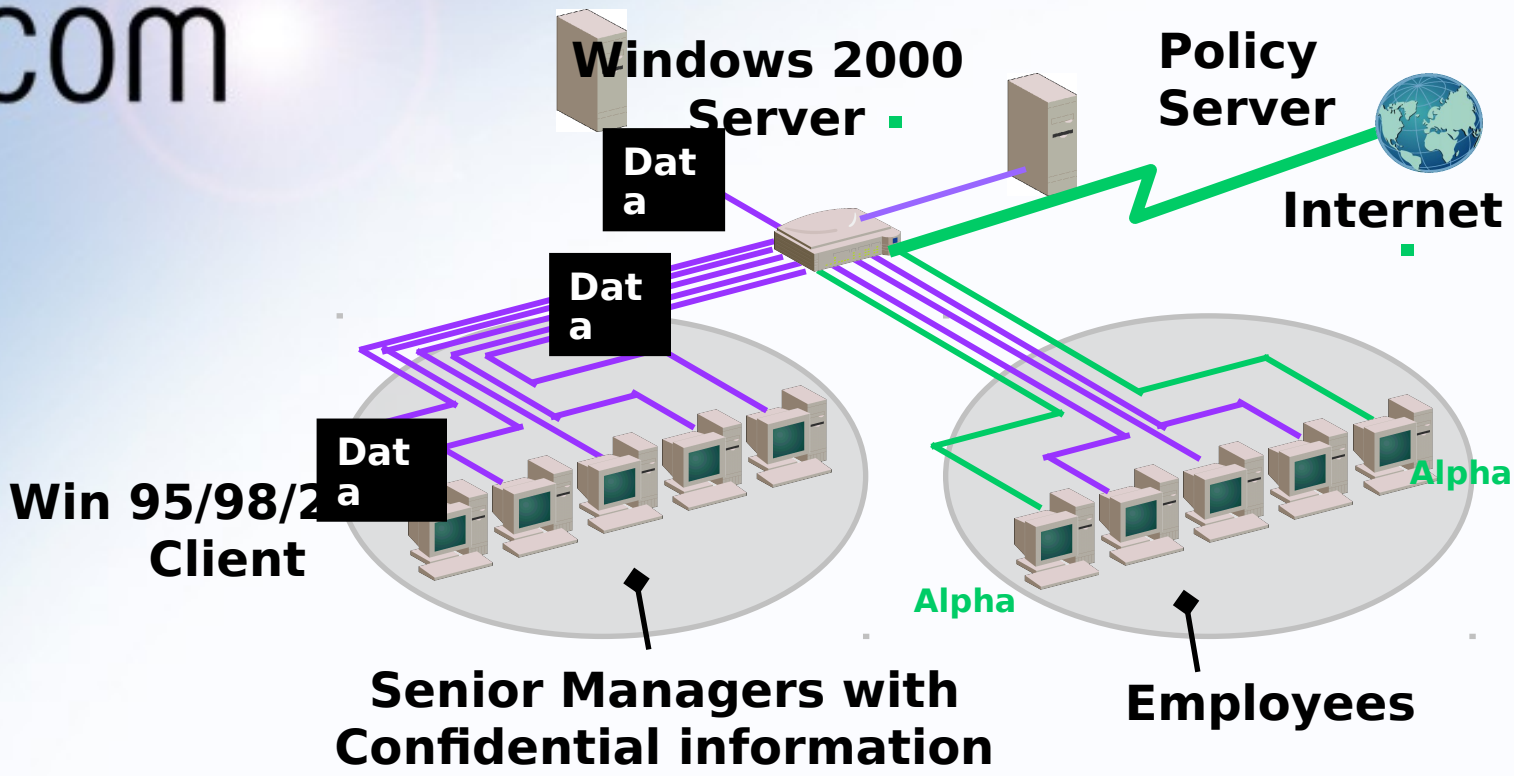
Embedded Firewall Applications

No Sniffing



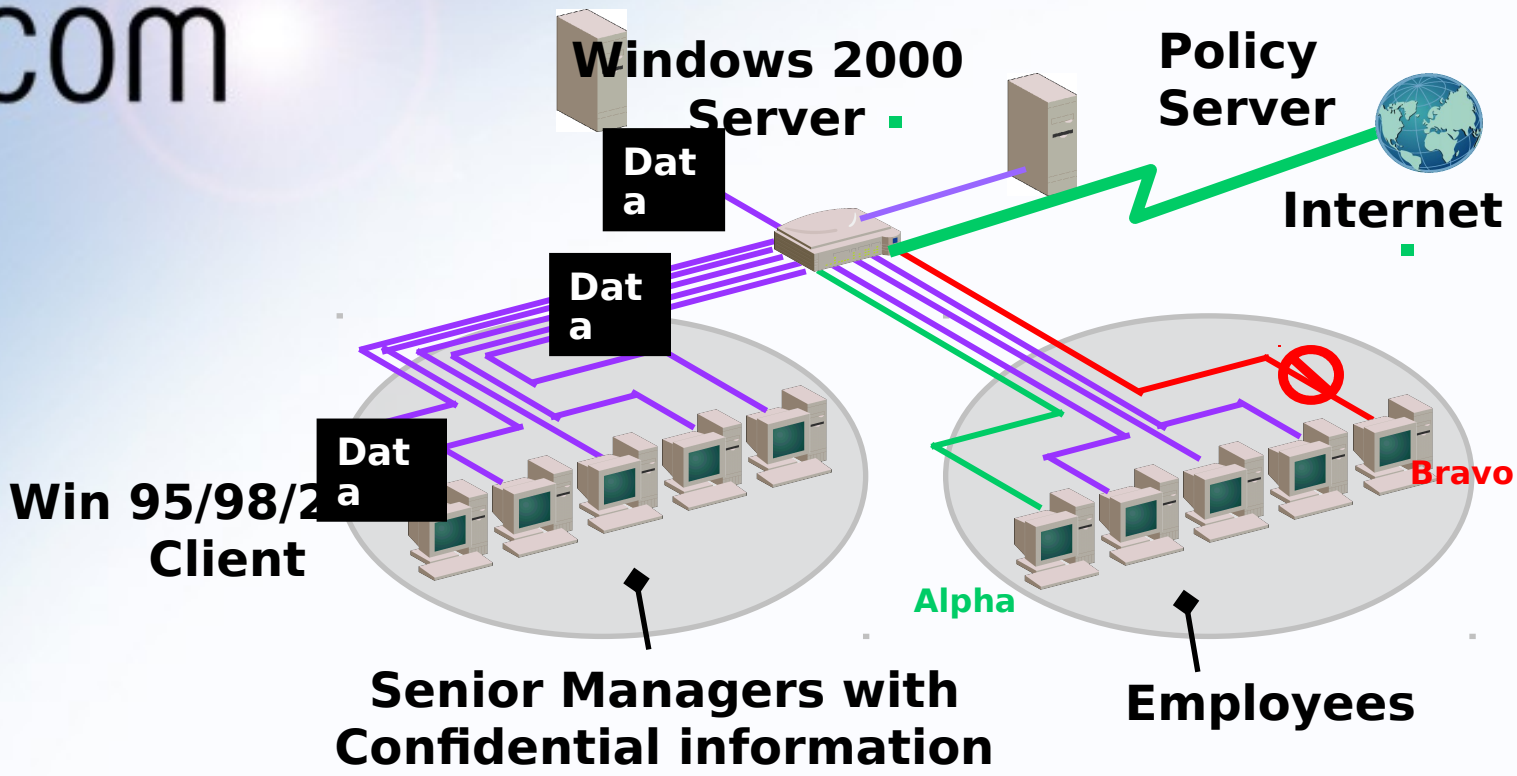
- Good insider logs into Telnet server
- Bad insider sniffs the password from the LAN
- No sniffing policy is pushed
  - **Hostile insider is unable to sniff passwords**

THREATCON Alpha



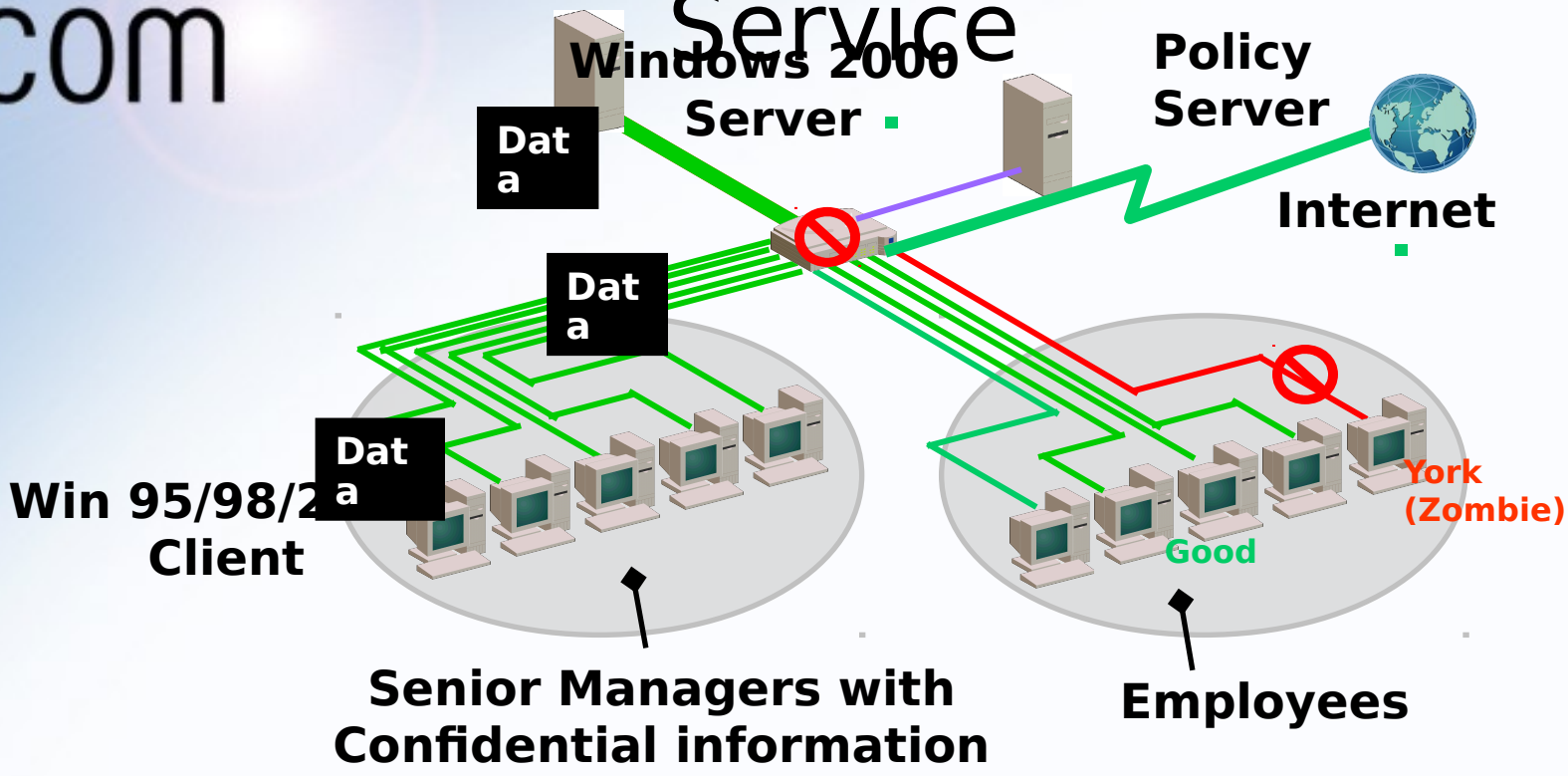
- Protocols and/or addresses can be restricted on a per host basis as INFOCON changes
  - Block all port x traffic to a user's machine
  - Block a service from a specific subnet

THREATCON Bravo



- Each host can be at a different INFOCON level
- Changing INFOCON is easy
  - No user action required
  - No rebooting required

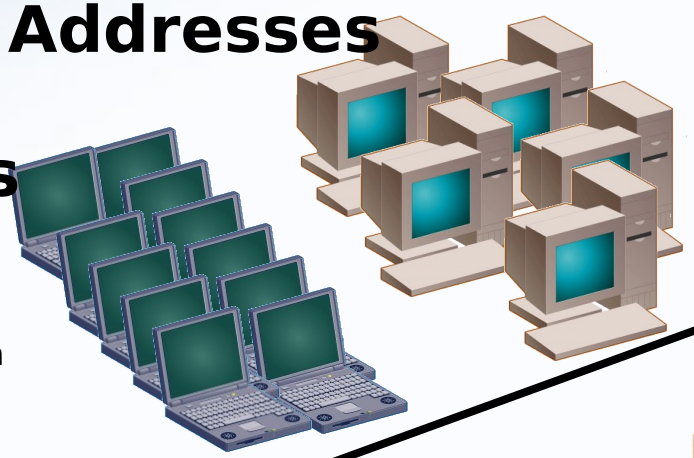
No Denial of Service



- York is a zombie launching a DDOS attack against the server
  - Good insiders cannot access the server
- "Block all" policy is pushed to the zombie
  - Service is restored to good users

The Internal Network: Uncontrolled Inventory

IP Addresses

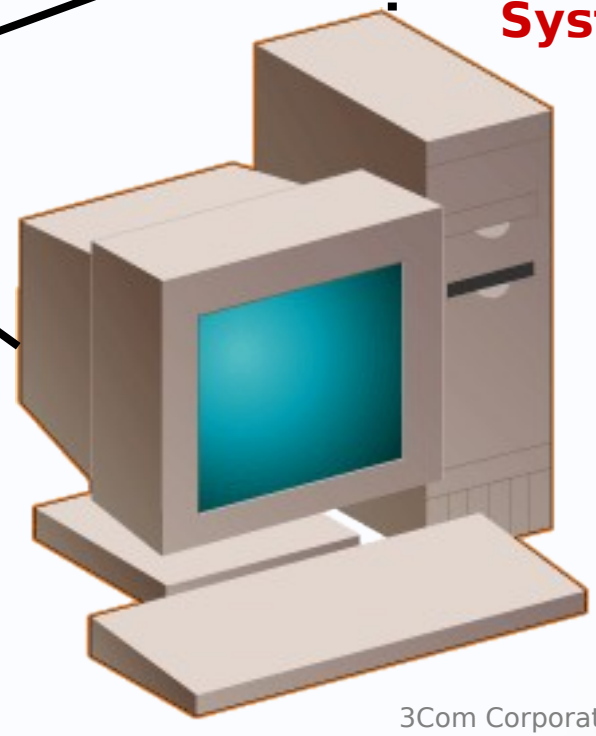


illions of Ports & Protocols are allowed in and out of this Network

Ports/Protocols

	Message Send Protocol
SQL	FTP (Port 21)
Bootstrap	SSH remote login
TFTP	Telnet
Finger	SMTP (mail)
HTTP(Port 80)	Host name server
Sun RPC	Login host protocol
NetBIOS	Domain name server
SNMP	
Internet relay chat	
HTTP management...	

Unprotected System



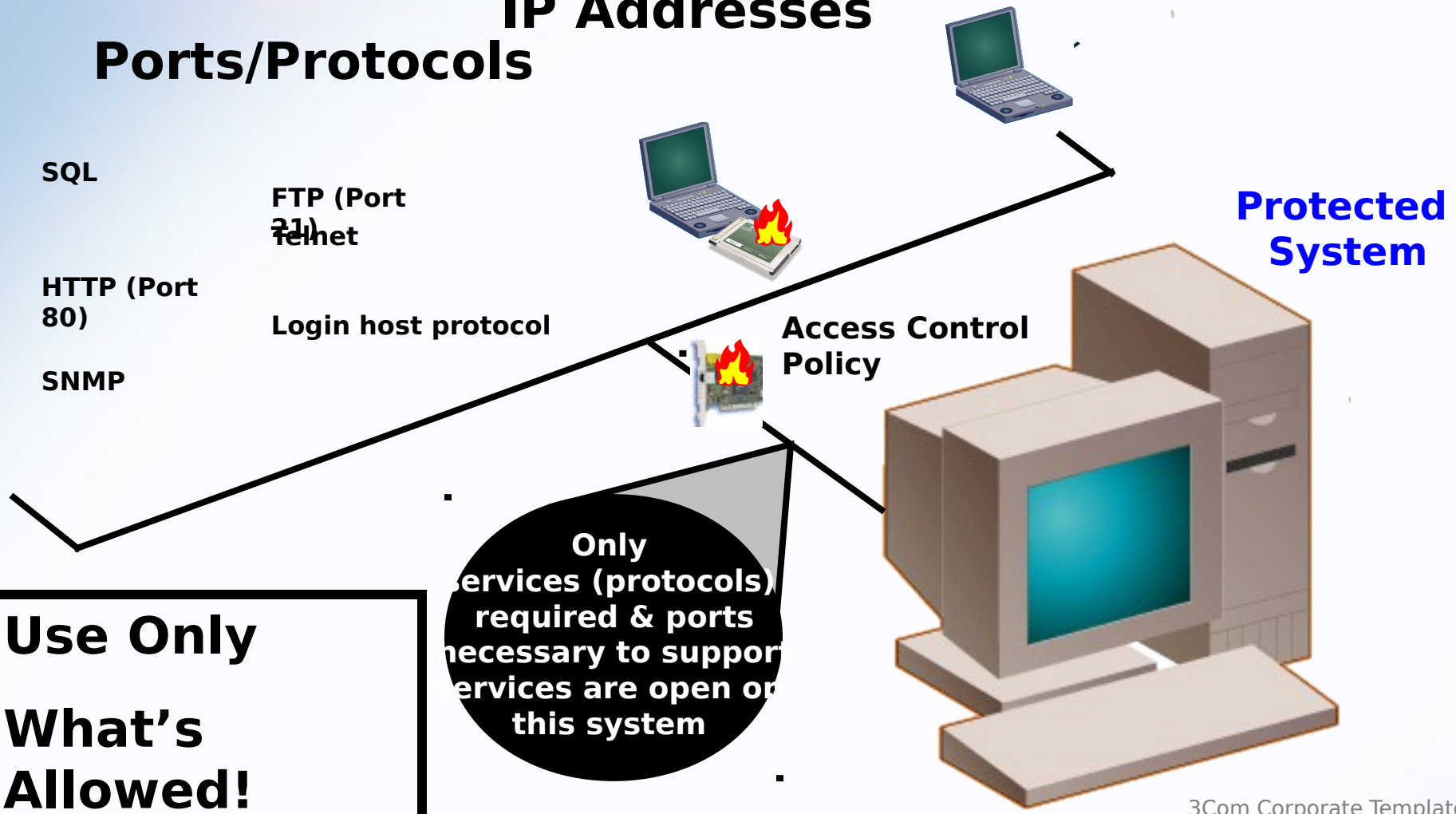
64,000 Ports & Dozens of Protocols are allowed in and out of this system

Leave Everything Open – Use Whatever You Want. Anyone Can Attach.

Asset Control – Defined by Security Administrator

IP Addresses

Ports/Protocols

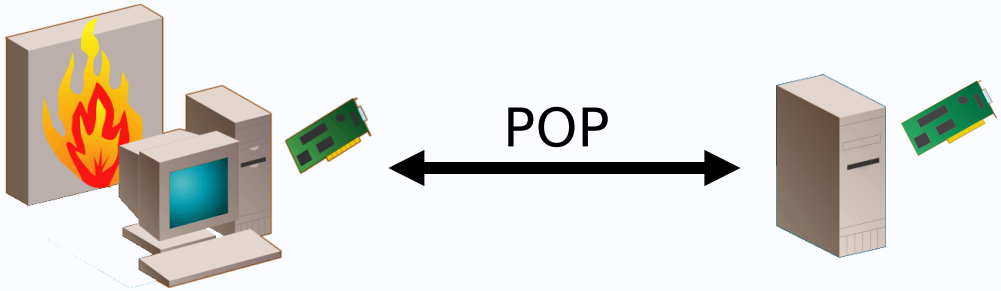


Use Only

What's Allowed!

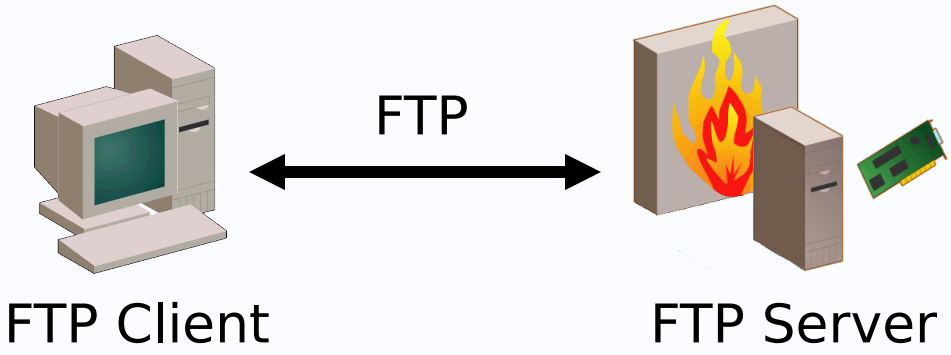
Contractor Workstation: E-mail Access

- On workstation, enforce the following rules:
  - Allow access to/from IP address of e-mail server
  - Allow port 110 for POP traffic
  - Deny all other traffic



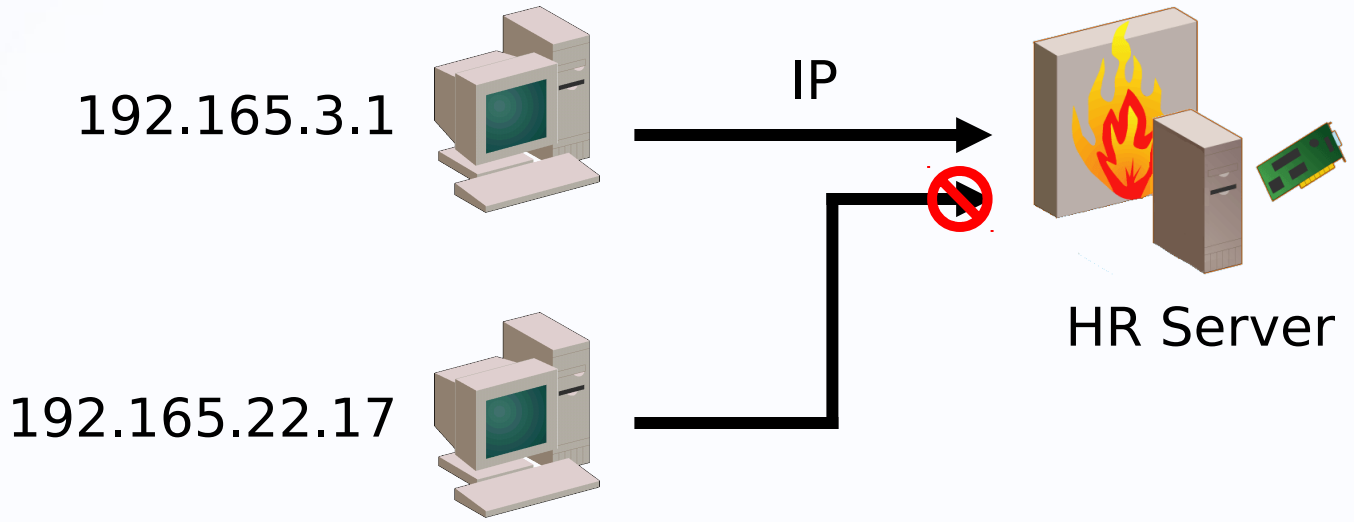
Hardened FTP Server

- On FTP server, enforce the following rules:
  - Use Windows 2000 pre-defined rule set
  - Use FTP Server pre-defined rule set to allow the host to accept/provide file transfers using FTP
  - Deny all other traffic



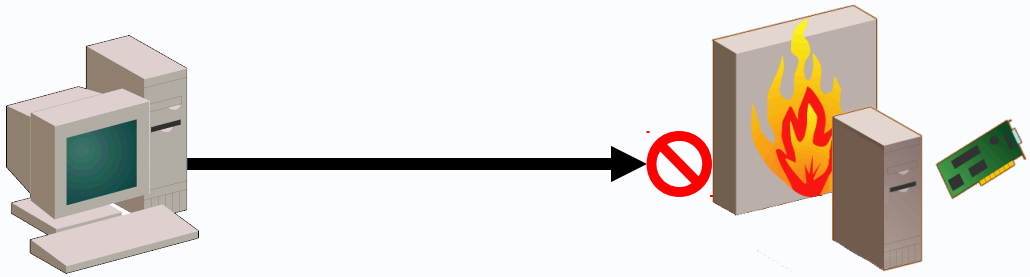
Sensitive Information Server

- On server, enforce the following rules:
  - Same rules as Hardened Server
  - Allow traffic to/from specified IP addresses
  - Deny all other traffic



Network Attack Response (In Real Time)

- If an attack is detected, IT administrator can:
  - Block outgoing traffic from attacking host
  - Block all traffic on critical servers to prevent further damage/proliferation of attack
  - Block protocols or ports used in attack



Attacking Host

Compromised Server

Summary

- Need-to-know policies can be enforced at each node in real-time
- 3Com Embedded Firewall is tamper-resistant - embedded in the NIC and independent of the operating system
- Provides security on both servers (extranets) and hosts.
- Auditing enhances intrusion detection
- Complements the Perimeter Firewall
- Centrally managed and controlled – transparent to the user
- Remote/traveling user support
- Supported by DARPA (Defense Advanced Research Projects Agency).

Embedded Firewalls Meet Today's Security Challenges

- Provides protection for every computer
- Know who's on your network
- Stops hackers at the most likely point of entry, the network connection
- Provides managed security controls
- Protects your valuable network assets
- Distinguishes users based on role or function, not "outsider" versus "insider"

Distributed Embedded Firewalls are complementary to existing network-centric solutions, enabling a "Defense in Depth" strategy

For more information, please visit www.3com.com

3com

Possible made practical™